# EXHIBIT F

19MAG 7563

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information Associated with the iCloud Account with Apple ID [redacted] Maintained at Premises Controlled by Apple Inc., USAO Reference Nos. [redacted] and [redacted]

# SEARCH WARRANT

TO: Apple, Inc. ("Provider")

United States Attorney's Office for the Southern District of New York and Federal Bureau of Investigation (together, the "Investigative Agencies")

**1. Warrant.** Upon an affidavit of DeLeassa Penland, Special Agent with the United States Attorney's Office for the Southern District of New York, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the Apple iCloud account associated with the Apple ID [redacted] maintained at premises controlled by Apple Inc., contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agencies, within 14 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within seven days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**2. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

Aug. 13, 2019
Date Issued

5:15 p.m.
Time Issued

Paul G. Gardephe
HON. PAUL G. GARDEPHE
UNITED STATES DISTRICT JUDGE
SOUTHERN DISTRICT OF NEW YORK

**Attachment A**

**I. Subject Account and Execution of Warrant**

This warrant is directed to Apple Inc. ("Apple" or the "Provider"), headquartered at 1 Infinite Loop in Cupertino, California, and applies to all content and other information within the Provider's possession, custody, or control associated with the Apple iCloud account for the Apple ID [redacted] (the "Subject Account"). A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

**II. Information to be Produced by the Provider**

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account from March 1, 2018 through March 26, 2019:

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Message content.* All messages sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message).

b. *Images and videos.* All pictures and videos posted and/or stored by an individual using the account, including metadata and geotags.

c. *Address book information.* All friend list, address book, contact list, or similar information associated with the Subject Account.

d. *Other stored electronic information.* All records and other information stored by the Subject Account's user, including data from third-party apps.

e. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

f. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

g. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

h. *Find My iPhone and Remote Deletion Activity*: All find My iPhone connection logs and Find My iPhone transactional activity for requests to remotely lock or erase or wipe a device.

i. *Device Backups*. All versions of iOS device backups associated with or stored within the Subject Account, whether made manually or automatically.

j. *Preserved records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise, including data preserved pursuant to a request assigned the reference numbe[redacted]

k. *Encryption keys.* Any and all "keybag" and "FileInfoList.txt" files associated with any device backups in the Subject Account.

## III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside vendors or technical experts under government control) are authorized to review the records produced by the Provider (a) for the time period of on or about August 1, 2018 through March 25, 2019, in order to locate any evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 875(d) (transmitting interstate communications with intent to extort) and 1951 (extortion), and a conspiracy and/or attempt to commit the same, arising from a scheme in which MICHAEL AVENATTI and [redacted] used interstate communications and threats of economic harm in an attempt to obtain payments from [redacted] n or about March 2019 (collectively, the "Extortion Offenses") and (b) for the time period of on or about March 1, 2018 through February 28, 2019, in order to locate any evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 1028A (aggravated identity theft), 1341 (mail fraud), 1343 (wire fraud), 1956 (money laundering), and 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and an attempt to commit the same, relating to a scheme executed by AVENATTI between in or about March 2018 and February 2019 to defraud one of his then-clients, [redacted] including by creating a document ostensibly "signed" by [redacted] directing that [redacted] literary agent send significant payments to AVENATTI instead of [redacted] without [redacted] permission (collectively, the "Fraud Offenses"), including as follows:

f. Evidence concerning the identity or location of the owner or use of the Subject Account, such as internet protocol address or other similar information associated with logins,

registration information, default signature, textual references to the name or identity of the user of the device, textual references to the past, present, or future location of the user of the device, self-taken photographs, and communications with Apple concerning the Subject Account.

g. Evidence of communications or documents involving [redacted] any of its employees, agents, or representatives, [redacted] relating to the commission of the Extortion Offenses, such as text messages or emails between AVENATTI, [redacted] and [redacted] employees, agents, or representatives, that relate to demands for payments; allegations concerning wrongdoing by [redacted] or its employees; or threats to publicize alleged wrongdoing by [redacted] or its employees.

h. Evidence relating to payments to or from [redacted] or their agents or legal representatives, including any documentation concerning payments of [redacted]'s book advance from [redacted] and any communications related to such payments, relating to the commission of the Fraud Offenses, such as text messages or emails concerning the advance payments associated with [redacted]'s book.

i. Evidence of communications with or regarding [redacted] or their agents or legal representatives, including any communications concerning payments to AVENATTI or [redacted], relating to the commission of the Fraud Offenses, such as text messages or emails concerning [redacted]'s book contract, the advance payments associated with [redacted]'s book, or the publicity efforts and sales of [redacted]'s book.

j. Evidence of deposits, withdrawals, wire transfers, and other movements of money between bank accounts; communications concerning financial transactions, including with financial institutions; and financial records concerning the existence, disposition, transfer, and movement of money and other assets, such as copies of bank statements, email communications with financial institutions, or lists of assets or transactions.

* * *

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.